

Hybrid Noncoherent Network Coding

Vitaly Skachek, Olgica Milenkovic, Angelia Nedić

University of Illinois, Urbana-Champaign
1308 W. Main Street, Urbana, IL 61801, USA

Abstract

We describe a novel extension of subspace codes for noncoherent networks, suitable for use when the network is viewed as a communication system that introduces both dimension and symbol errors. We show that when symbol erasures occur in a significantly large number of different basis vectors transmitted through the network and when the min-cut of the networks is much smaller than the length of the transmitted codewords, the new family of codes outperforms their subspace code counterparts.

For the proposed coding scheme, termed hybrid network coding, we derive two upper bounds on the size of the codes. These bounds represent a variation of the Singleton and of the sphere-packing bound. We show that a simple concatenated scheme that represents a combination of subspace codes and Reed-Solomon codes is asymptotically optimal with respect to the Singleton bound. Finally, we describe two efficient decoding algorithms for concatenated subspace codes that in certain cases have smaller complexity than subspace decoders.

1 Introduction

Network coding is a scheme introduced by Ahlswede *et al.* [1] for efficient communication over networks with transmission bottlenecks. The authors of [1] showed that under broadcast scenario in networks, the maximal theoretically achievable communication rate – called the *capacity* of the network – can be characterized by minimal cuts in the network and achieved by appropriate coding methods.

In the last decade, network coding became a focal point of research in coding theory. There exists a variety of network coding solutions currently used in practice. A random network coding approach was first proposed in [9], while algebraic coding was shown to achieve the capacity of a class of networks in [15, 14]. Non-linear approaches were also studied in [3]. The use of network coding for error correction was first proposed in [2]. When

the network topology is not known, or when it changes with time, it was suggested in [13] to use subspace coding for joint error correcting and network coding.

In our work, we follow the line of research started in [13]. More specifically, we consider error-correction for a special case of network coding, suitable for practical applications in which the topology of the network is not known or changes with time. This type of scheme is, as already mentioned, known as coding for **noncoherent networks**. Currently, the only known approach for noncoherent network coding utilizes subspace codes.

Subspace codes for noncoherent network coding are based on the idea that the transmitted data vectors can be associated with linear vector subspaces. Linear network coding does not change the information about the subspaces, since it only allows for linear combining of the transmitted bases vectors. Hence, if there are no errors, the receiver obtains uncompromised information regarding the transmitted subspace. The transmitted subspaces can only be modified within the network through the introduction of errors. In order to protect the transmitted information in the latter case, one has to add carefully structured redundancy into the subspace messages.

In the context of the work [13], the errors are modeled as **dimension gains** and **dimension losses**. These notions, although of theoretical value, may appear rather abstract in real networking applications, where packets (symbols or collections of symbols) are subjected to erasures or substitution errors. One fundamental question remains: how is one to interpret the notion of dimension gains and losses in terms of symbol errors and erasures, and what kind of errors and erasures constitute dimension gains and losses?

We propose a **hybrid approach** to noncoherent network coding, which attempts to connect the notions of dimension loss and gain with those of individual symbol errors and erasures. The crux of our approach is to consider network coding where dimension gains and losses, in addition to individual symbol errors and erasures, are all possible. This allows us to study the trade-offs between the required overhead in the network layer aimed at correcting dimension gains/losses, and the overhead in the physical layer designated to correcting symbol erasures and errors.

Our main result shows that by incorporating symbol error correcting mechanism into subspace codes, one can increase the number of tolerable dimension gains and losses, without compromising the network throughput. Hence, the proposed approach leads to an increase in the overall number of correctable errors in the subspace-based scheme akin to [13].

In order to illustrate our approach, consider the following straightforward example. Assume the case of a noncoherently coded network in which arbitrary (unknown) ten symbols are erased from the basis vectors representing the message. The first question is how many dimension losses should be considered in the model of [13]? One reasonable way to look at it is to assume the worst-case scenario when each symbol erasure introduces one dimension loss, and each error introduces a simultaneous dimension loss and gain. Consequently, ten symbol erasures would amount to ten dimension losses. However, if there were an alternative

way to correct some of these symbol erasures or errors, the effective number of dimension losses and gains may become significantly smaller. In the example, correcting five symbol erasures would, in the best case, reduce the burden of subspace codes in terms of dimension loss recovery by five dimensions.

We therefore pose the following questions: what are the fundamental performance bounds for noncoherent network coding schemes, consequently termed hybrid network codes, capable of correcting symbol erasures and errors on one side, and dimension gains and losses on the other side? What is the optimal rate allocation scheme for hybrid network codes in terms of dimension losses/gains and symbol errors/erasures? What is the optimal ratio between the two allocation rates and how can it be achieved practically? How does one efficiently correct errors in this new scheme? The work in this paper is aimed at answering these questions.

There are various potential applications for the proposed network codes. The hybrid codes can be useful in networks, where no link-layer error correction is performed. Such networks include sensor networks, where the computational power of the intermediate nodes is not sufficient to perform error correction at every such node. The hybrid codes can also be used in the networks, where the size of a physical layer packet is very small, and where the network layer packet consists of many physical layer packets. Then, any physical layer packet can be regarded as a single symbol.

The paper is organized as follows. The notation and prior work are discussed in Section 2. In the sections that follow, we define hybrid codes that can be used for simultaneous correction of dimension losses/gains and symbol erasures in noncoherent networks. More specifically, the basic code requirements and parameters are presented in Section 3. Two upper bounds on the size of hybrid codes, the Singleton bound and the sphere-packing bound, are presented in Section 4. A straightforward code construction appears in Section 5.1. The analysis of code parameters and the comparison with known subspace code constructions also appear in the same section. The decoding algorithm for the proposed codes is presented in 6. In the Appendix we show that the same codes can also be used for simultaneous correction of dimension losses and symbol erasures/errors. We state some results analogous to those in Sections 3-6. Finally, we discuss some results related to simultaneous correction of both dimension losses/gains and symbol erasures/errors.

2 Notation and Prior Work

Let W be a vector space over a finite field \mathbb{F}_q and let $V, U \subseteq W$ be linear subspaces of W . We use the notation $\dim(V)$ for the dimension of V . We denote the sum of two subspaces U and V as $U + V = \{\mathbf{u} + \mathbf{v} : \mathbf{u} \in U, \mathbf{v} \in V\}$. If $U \cap V = \emptyset$, then for any $\mathbf{w} \in U + V$ there is a unique representation in terms of the sum of two vectors $\mathbf{w} = \mathbf{u} + \mathbf{v}$, where $\mathbf{u} \in U$ and $\mathbf{v} \in V$. In this case we say that $U + V$ is a direct sum, and denote it by $U \oplus V$. It is easy to check that $\dim(U \oplus V) = \dim(U) + \dim(V)$.

Let $W = U' \oplus U''$. For $V \subseteq W$ we define a projection of V onto U' , denoted by $V|_{U'}$, as follows:

$$V|_{U'} = \{\mathbf{u}_1 : \mathbf{u}_1 + \mathbf{u}_2 \in V, \mathbf{u}_1 \in U', \mathbf{u}_2 \in U''\}.$$

Similarly, we denote the projection of the vector \mathbf{u} onto U' by $(\mathbf{u})|_{U'}$. For two vectors, \mathbf{u} and \mathbf{v} , we write $\mathbf{u} \cdot \mathbf{v}$ to denote their scalar product. If $W = U' \oplus U''$ and for all $\mathbf{u} \in U'$, $\mathbf{v} \in U''$ it holds $\mathbf{u} \cdot \mathbf{v} = 0$ (i.e. U' and U'' are orthogonal), we also write $W = U' \odot U''$.

For a set of vectors $S \subseteq W$, we use $\langle S \rangle$ to denote the linear span of the vectors in S . We also use the notation $\langle \mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_\ell \rangle$ for a vector span of the set of vectors $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_\ell\}$. Let \mathbb{N} be the set of the positive integer numbers. We write $\mathbf{0}^m$ to denote the all-zero vector of length m , for any $m \in \mathbb{N}$. When the value of m is clear from the context, we sometimes write $\mathbf{0}$ rather than $\mathbf{0}^m$. We also denote by $\mathbf{e}_i \triangleq (\underbrace{0, \dots, 0}_{i-1}, 1, \underbrace{0, \dots, 0}_{n-i}) \in \mathbb{F}_q^n$ a unity vector

which has a one in position $i \in \mathbb{N}$ and zeros in all other positions. The length of the vector will be clear from the context.

Assume that $\dim(W) = n$. We use the notation $\mathcal{P}(W, \ell)$ for the set of all subspaces of W of dimension ℓ , and $\mathcal{P}(W)$ for the set of all subspaces of W of any dimension. The number of ℓ -dimensional subspaces of W , $0 \leq \ell \leq n$, is given by the q -ary Gaussian coefficient (see [24, Chapter 24]):

$$|\mathcal{P}(W, \ell)| = \begin{bmatrix} n \\ \ell \end{bmatrix}_q = \prod_{i=0}^{\ell-1} \frac{q^{n-i} - 1}{q^{\ell-i} - 1}.$$

For $U, V \in W$,

$$\mathbf{D}(U, V) = \dim(U) + \dim(V) - 2 \dim(U \cap V)$$

be a distance measure between U and V in the Grassmanian metric (see [13]). We use the notation $\mathbf{d}(\mathbf{u}, \mathbf{v})$ for the Hamming distance between two vectors \mathbf{u} and \mathbf{v} of the same length.

We say that the code \mathbb{C} is an $[n, \ell, \log_q(M), D]_q$ subspace code, if it represents a collection of subspaces in an ambient space W over \mathbb{F}_q , which satisfies the following conditions:

1. W is a vector space over \mathbb{F}_q and $\dim(W) = n$;
2. for all $V \in \mathbb{C}$, $\dim(V) = \ell$;
3. $|\mathbb{C}| = M$;
4. for all $U, V \in \mathbb{C}$, $U \neq V$, it holds that $\dim(U \cap V) \leq \ell - D$, so that consequently $\mathbf{D}(U, V) \geq 2D$.

A *linearized polynomial* is a polynomial of the form

$$L(x) = \sum_{i=0}^{k-1} L_i x^{q^i},$$

where all $L_i \in \mathbb{F}$. It can be easily checked that linearized polynomial is a linear transformation from a vector space associated with \mathbb{F} into itself.

Given these definitions, we recall the construction in [13]. Let $\mathbb{F} = \mathbb{F}_{q^m}$ be an extension field of \mathbb{F}_q , $m > 1$. Then, \mathbb{F} is a vector space over \mathbb{F}_q . Let $\{\alpha_1, \alpha_2, \dots, \alpha_\ell\} \subseteq \mathbb{F}$ be a set of ℓ linearly independent elements in \mathbb{F} , and let

$$A \triangleq \langle \alpha_1, \alpha_2, \dots, \alpha_\ell \rangle ,$$

and

$$W \triangleq A \oplus \mathbb{F} = \{(\mathbf{v}_1, \mathbf{v}_2) : \mathbf{v}_1 \in A, \mathbf{v}_2 \in \mathbb{F}\} . \quad (1)$$

Note that we wrote $\mathbf{v} \in W$ as $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2)$, where $\mathbf{v}_1 \in \langle A \rangle$ and $\mathbf{v}_2 \in \mathbb{F}$ (consequently, the vector \mathbf{v} can be viewed as an $(\ell + m)$ -tuple over \mathbb{F}_q , where the first ℓ symbols in \mathbb{F}_q describe the coordinates of \mathbf{v}_1 , and the last m symbols describe the coordinates of \mathbf{v}_2). For a vector space $V \subseteq W$ we define as before

$$V|_{\mathbb{F}} = \{\mathbf{v}_2 \in \mathbb{F} : (\mathbf{v}_1, \mathbf{v}_2) \in V\} .$$

Let $\mathbb{F}^k[x]$ denote the set of linearized polynomials $f(x)$ over \mathbb{F} of degree at most q^{k-1} , $k \geq 1$. Define the mapping $\mathcal{E} : \mathbb{F}^k[x] \rightarrow \mathcal{P}(W, \ell)$ as

$$\mathcal{E}(f(x)) = \langle (\alpha_1, f(\alpha_1)), \dots, (\alpha_\ell, f(\alpha_\ell)) \rangle .$$

Using linearized polynomials, one can introduce a code \mathcal{K} (for $k \leq \ell$) as a collection of subspaces of the form [13]

$$\mathcal{K} = \{\mathcal{E}(f(x)) : f(x) \in \mathbb{F}^k[x]\} . \quad (2)$$

The code \mathcal{K} can be easily shown to be an $[\ell + m, \ell, mk, \geq 2(\ell - k + 1)]_q$ subspace code [13].

To formalize the network model, the authors of [13] also introduced the *operator channel* and erasure operator as follows. Let $k \geq 0$ be an integer. Given a subspace $V \subseteq W$, if $\dim(V) \geq k$ the stochastic *erasure operator* $\mathcal{H}_k(V)$ returns some random k -dimensional subspace of V . Otherwise it returns V itself. Then, for any subspace U in W , it is always possible to write $U = \mathcal{H}_k(V) \oplus E$, where $\mathcal{H}_k(V)$ is a realization of $U \cap V$ and E is a subspace of W .

Decoding algorithms for the code \mathcal{K} were presented in [13] and [20]. Suppose that $V \in \mathcal{K}$ is transmitted over the operator channel. Suppose also that an $(\ell - \kappa + \gamma)$ -dimensional subspace U of W is received, where $k = \dim(U \cap V) = \ell - \kappa$. Here $\kappa = \ell - k$ denotes the number of dimension losses when modifying the subspace V to $V \cap U$, while γ similarly denotes the number of dimension insertions needed to transform $V \cap U$ into U . Note that $\dim(E) = \gamma$, where E is given in the decomposition of U . The decoders, presented in [13] and [20], are able to recover a single $V \in \mathcal{K}$ whenever $\kappa + \gamma < \ell - k + 1$. We denote hereafter a

decoder for the code \mathcal{K} described in [13] and [20] by $\mathcal{D}_{\mathcal{K}}$. Note that the decoding complexity of $\mathcal{D}_{\mathcal{K}}$ is polynomial both in the dimension of the ambient vector space and the subspace distance D .

We find the following lemma useful in our subsequent derivations.

Lemma 2.1. *Let $W = U' \oplus U''$ be a vector space over \mathbb{F}_q , and let $V_1, V_2 \subseteq W$ be two vector subspaces. Then*

$$D(V_1, V_2) \geq D(V_1|_{U'}, V_2|_{U'}) .$$

Proof. By definition,

$$D(V_1, V_2) = (\dim(V_1) - \dim(V_1 \cap V_2)) + (\dim(V_2) - \dim(V_1 \cap V_2)) .$$

Let $s = \dim(V_1 \cap V_2)$ and $t = \dim(V_1) - \dim(V_1 \cap V_2)$. Take $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_s\}$ to be a basis of $V_1 \cap V_2$ and $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_t\}$ to be t linearly independent vectors in $V_1 \setminus V_2$. Then, $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_s\}$ and $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_t\}$ jointly constitute a basis of V_1 .

Next, consider $(V_1 \cap V_2)|_{U'} = \langle (\mathbf{v}_1)|_{U'}, (\mathbf{v}_2)|_{U'}, \dots, (\mathbf{v}_s)|_{U'} \rangle$. Clearly, $(V_1 \cap V_2)|_{U'}$ is a subspace of $V_1|_{U'}$ and of $V_2|_{U'}$. Therefore,

$$(V_1 \cap V_2)|_{U'} \subseteq V_1|_{U'} \cap V_2|_{U'} .$$

Note that the inclusion in the above relation may be strict.

On the other hand, \mathcal{B}_1 together with $\{(\mathbf{u}_1)|_{U'}, (\mathbf{u}_2)|_{U'}, \dots, (\mathbf{u}_t)|_{U'}\}$ spans $V_1|_{U'}$. We thus have that

$$\dim(V_1|_{U'}) - \dim(V_1|_{U'} \cap V_2|_{U'}) \leq \dim(V_1|_{U'}) - \dim(\mathcal{B}_1) \leq t = \dim(V_1) - \dim(V_1 \cap V_2) . \quad (3)$$

Similarly to (3), it can be shown that

$$\dim(V_2|_{U'}) - \dim(V_1|_{U'} \cap V_2|_{U'}) \leq \dim(V_2) - \dim(V_1 \cap V_2) . \quad (4)$$

From (3) and (4), we obtain that

$$\begin{aligned} D(V_1|_{U'}, V_2|_{U'}) &= (\dim(V_1|_{U'}) - \dim(V_1|_{U'} \cap V_2|_{U'})) + (\dim(V_2|_{U'}) - \dim(V_1|_{U'} \cap V_2|_{U'})) \\ &\leq (\dim(V_1) - \dim(V_1 \cap V_2)) + (\dim(V_2) - \dim(V_1 \cap V_2)) \\ &= D(V_1, V_2) . \end{aligned}$$

This completes the proof of the claimed result. \square

3 Hybrid Coding for Symbol Erasures and Dimension Gains/Losses

3.1 Motivation

Noncoherent network coding makes the topology of the network transparent to the code designer, and it has a strong theoretical foundations. Nevertheless, there are some practical issues that remain to be taken into account when applying this coding scheme. First, the notion of “dimension loss” is fairly abstract since in networks only symbols (packets) can be erased or subjected to errors. It is reasonable to assume that a dimension loss corresponds to a number of symbol erasures/errors within the same message, although it is not clear how large this number is supposed to be. In the worst case scenario, even one symbol error may lead to the change of one dimension. Second, the achievable throughput of the scheme and the underlying decoding complexity may be significantly inferior to those achievable only through classical network coding. Of course, this claim only holds if the error-correcting scheme is integrable with a linear network coding method.

Let $W_{\mathcal{L}}$ denote the space \mathbb{F}_q^n for some $n \in \mathbb{N}$ and let \mathcal{L} be a collection of subspaces of $W_{\mathcal{L}}$ of dimension ℓ . Assume that $V \in \mathcal{L}$ is transmitted over a noncoherent network. Assume also that ρ symbol errors and μ symbol erasures happened to any of the vectors of V , while they were propagating through the network. Denote by U the subspace spanned by the vectors obtained at the destination.

Then, the vectors observed by the receiver are linear combinations of the vectors in V . Each of these vectors has, in the worst case scenario, at most ρ symbol errors and μ symbol erasures. Indeed, this can be justified as follows. If some vector \mathbf{x} was transmitted in the network, and an erasure (or error) occurred in its j -th entry, in the worst case scenario this erasure (error) can effect only the j -th coordinates in *all* vectors in U , causing this coordinate to be erased (or altered, respectively) in all of them. This is true for any network topology. Such erasure (or error) does not effect any other entries in the vectors observed by the receiver.

This observation motivates the following definitions.

Definition 3.1. Consider a vector space $U \subseteq W_{\mathcal{L}}$. Write $W_{\mathcal{L}} = W_S \odot \langle \mathbf{e}_j \rangle$ for some $1 \leq j \leq n$. A symbol error in coordinate j of U is a mapping from U to $U' \subseteq W_{\mathcal{L}}$, such that

$$U \neq U' \quad \text{and} \quad U|_{W_S} = U'|_{W_S} .$$

Definition 3.2. Let $U \subseteq W_{\mathcal{L}}$ and assume that $W_{\mathcal{L}} = W_S \odot \langle \mathbf{e}_j \rangle$. A symbol erasure in coordinate j of U is a mapping from U to $U' \subseteq W_S$, such that

$$U|_{W_S} = U' .$$

Observe, that symbol errors and erasures can be combined. Thus, we say that the vector space U' is obtained from U by ρ symbol errors and μ symbol erasures, if there exist a series of ρ error mappings and μ erasure mappings as above from U to U' . Note that under these definitions, the order of errors is irrelevant. Thus, if U' is obtained from U by errors in the coordinates $\{j_1, j_2, \dots, j_\rho\}$ of U and erasures in the coordinates $\{j'_1, j'_2, \dots, j'_\tau\}$ of U , then any order of application of error and erasure mappings yields the same subspace U' .

We summarize the above discussion by mentioning that there are four potential types of data errors in a network that are not necessarily incurred independently:

1. Symbol erasures;
2. Symbol errors;
3. Dimension losses;
4. Dimension gains.

In the forthcoming sections of this paper, we concentrate on designing codes that are able to handle simultaneously symbol erasures, dimension losses and dimension gains. We postpone the discussion about how to handle symbol errors to the Appendix.

3.2 Code Definition

We start the development with the following definition.

Definition 3.3. *A subspace code $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}}, \ell)$ (a collection of subspaces in $W_{\mathcal{L}}$ of dimension ℓ) is called a code correcting $d - 1$ symbols erasures and $D - 1$ dimension errors or a (d, D) hybrid code if it satisfies the following properties:*

1. *For any $U \in \mathcal{L}$, $\dim(U) = \ell$.*
2. *For any $U, V \in \mathcal{L}$, $\dim(U) + \dim(V) - 2 \dim(U \cap V) \geq 2D$.*
3. *Let $V \in \mathcal{L}$. Let V' be the subspace obtained from V by μ symbol erasures, where $\mu \leq d - 1$. Then, for any possible combination of μ symbol erasures with $\mu \leq d - 1$, $\dim(V') = \ell$ and the space V is the only pre-image of V' in \mathcal{L} (under μ symbol erasures).*
4. *Let $U, V \in \mathcal{L}$. Let U', V' be obtained from U and V , respectively, by μ symbol erasures, where $\mu \leq d - 1$ (here both U and V have erasures in the same set of coordinates). Then, $\dim(U') + \dim(V') - 2 \dim(U' \cap V') \geq 2D$.*

Observe that condition (1) is a special case of condition (3), and (2) is a special case of condition (4), and therefore the first two conditions can be omitted. We kept these conditions for the sake of clarity.

We explain next why the class of hybrid (d, D) codes, satisfying (1)-(4), are termed **codes capable of correcting $d - 1$ symbol erasures and $D - 1$ dimension errors**.

Theorem 3.1. *Let $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}}, \ell)$ be a code satisfying (1)-(4). Then, \mathcal{L} is capable of correcting any error pattern of $d - 1$ symbol erasures and $D - 1$ dimension errors.*

Proof. Suppose that $V \in \mathcal{L}$ is transmitted through the operator channel, and that the subspace $U \in \mathcal{P}((\mathbb{F}_q)^{n-d+1}, \ell')$ is received, where $d - 1$ symbols erasures and $D - 1$ dimension errors have occurred. Note that here ℓ' is not necessarily equal to ℓ .

We assume without loss of generality that the dimension errors occurred first, and are followed by symbol erasures. As pointed out before, the order in which errors occur is irrelevant.

More formally, let $S = \{j_1, j_2, \dots, j_{d-1}\} \subseteq [n]$ be a set of erased coordinates in U , and let $W_{\mathcal{L}} = W_S \odot \langle \mathbf{e}_{j_1}, \mathbf{e}_{j_2}, \dots, \mathbf{e}_{j_{d-1}} \rangle$. Then,

$$U_1 = \mathcal{H}_k(V) \oplus E \quad \text{and} \quad U = U_1|_{W_S},$$

where $\dim(V \cap U_1) = k$, $\dim(U_1) = \ell'$, and $\ell + \ell' - 2k = D - 1$.

We show that if \mathcal{L} satisfies properties (1)-(4), then it is possible to recover V from U . Indeed, consider the following collection of subspaces

$$\mathcal{L}' = \{V|_{W_S} \subseteq (\mathbb{F}_q)^{n-d+1} : V \in \mathcal{L}\}.$$

Take any $V_1, V_2 \in \mathcal{L}'$. By property (3), $\dim(V_1) = \dim(V_2) = \ell$, and by property (4), $\dim(V_1) + \dim(V_2) - 2\dim(V_1 \cap V_2) = 2D$. Therefore, \mathcal{L}' is a $[n - d + 1, \ell, \log_q |\mathcal{L}|, 2D]_q$ subspace code. It is capable of correcting up to $D - 1$ dimension errors in $(\mathbb{F}_q)^{n-d+1}$.

Denote $V' = V|_{W_S} \in \mathcal{L}'$. Then, from Lemma 2.1,

$$D(V', U) \leq D(V, U_1) = D - 1.$$

We conclude that there exists a (not necessarily efficient) bounded-distance subspace decoder that is capable of recovering V' from U .

Finally, observe that V' is obtained from V by erasing $d - 1$ coordinates indexed by S . From property (3), the pre-image of V' under these erasures is unique. Therefore, V can be recovered from V' . \square

Henceforth, we use the notation $[n, \ell, \log_q(M), 2D, d]_q^1$ to denote the subspace code $\mathcal{L} \subseteq \mathcal{P}(W, \ell)$ with the following properties:

¹Whenever it is apparent from the context, we omit the subscript q .

1. $\dim(W) = n$;
2. for all $V \in \mathcal{C}$, $\dim(V) = \ell$;
3. $|\mathcal{L}| = M$;
4. \mathcal{L} is a code capable of correcting $d - 1$ symbols erasures and $D - 1$ dimension errors.

Remark 3.1. *The intuition behind the definition of hybrid codes is that dimension losses occur due to symbol erasures or errors. Symbol erasures are “easier” to correct than dimension losses, and upon correcting a number of symbol erasures one is expected to reduce the number of dimension losses. These claims are more rigorously formulated in Section 5.3.*

4 Bounds on the Parameters of Hybrid Codes

In this section, we develop the Singleton and the sphere-packing bound for hybrid codes handling dimension losses and gains, and symbol erasures simultaneously.

4.1 Singleton Bound

Assume that a vector space W over \mathbb{F}_q has dimension n , and let $\mathcal{L} \subseteq \mathcal{P}(W, \ell)$ be a subspace code. In what follows, we use a puncturing of the code \mathcal{L} , which is similar to symbol erasure in all $V \in \mathcal{L}$, but has a different assumption on the receiver’s knowledge. Specifically, we use the following definition.

Definition 4.1. *Puncturing of the code \mathcal{L} at position j is equivalent to the definition of erasure at coordinate j in Definition 3.2. The only difference is that in Definition 3.2 it is assumed that the receiver knows which coordinate was erased, while in this context no such knowledge is assumed.*

Theorem 4.1. *Let \mathcal{L} be a code of type $[n, \ell, \log_q(M), 2D, d]$ in the ambient space $W_{\mathcal{L}}$. If $d > 1$, then coordinate puncturing at coordinate j yields a code with parameters $[n - 1, \ell, \log_q(M), 2D, \geq d - 1]$.*

Proof. Let \mathcal{L}' be a code obtained by puncturing of the j -th coordinate in all vectors spaces in \mathcal{L} . Thus,

$$\mathcal{L}' = \{V' : \exists V \in \mathcal{L} \text{ and } V' \text{ is } V \text{ punctured in coordinate } j\} .$$

Clearly, the dimension of the ambient space decreases by one under this puncturing, and so the resulting space W' satisfies $\dim(W') = n - 1$.

Let $V \in \mathcal{L}$. Since $d > 1$, by property (3), $\dim(V') = \ell$ and V' has a unique pre-image. Therefore, $|\mathcal{L}| = |\mathcal{L}'|$.

The fourth parameter follows from the property that \mathcal{L} is a code correcting $d - 1$ symbol errors and $D - 1$ dimension errors. Thus, $\dim(U') + \dim(V') - 2 \dim(U' \cap V') \geq 2D$, where U' and V' are obtained by puncturing of U and V , respectively. The value of the last parameter follows from the fact that each subspace in \mathcal{L}' is obtained from its pre-image in \mathcal{L} by an erasure in the j -th coordinate. \square

Theorem 4.2. *The size M of the $[n, \ell, \log_q(M), 2D, d]_q$ code \mathcal{L} satisfies*

$$M \leq \mathcal{A}_q(n - d + 1, \ell, 2D),$$

where $\mathcal{A}_q(n, \ell, 2D)$ stands for the size of the largest subspace code $[n, \ell, M', 2D]_q$.

Proof. We apply $d - 1$ coordinate puncturings to \mathcal{L} . The resulting code has the same number of codewords as \mathcal{L} , and it is a set of ℓ dimensional subspaces in a $n - d + 1$ dimensional space, whose pairwise intersection is of dimension $\leq \ell - D$. In particular, its size is upper bounded by $\mathcal{A}_q(n - d + 1, \ell, 2D)$. \square

Corollary 4.3. *From the Singleton bound in [13], the size M of the $[n, \ell, \log_q(M), 2D, d]_q$ code \mathcal{L} satisfies*

$$M \leq \left[\begin{matrix} n - d - D + 2 \\ \ell - D + 1 \end{matrix} \right]_q. \quad (5)$$

We use the following result from [13].

Lemma 4.4 (Lemma 4 in [13]). *The Gaussian coefficient $\begin{bmatrix} n \\ \ell \end{bmatrix}_q$ satisfies*

$$1 < q^{-\ell(n-\ell)} \begin{bmatrix} n \\ \ell \end{bmatrix}_q < 4.$$

We also use the following definition of the rate of the subspace code.

Definition 4.2. *The rate of the subspace code \mathcal{L} is defined as $R = \frac{\log_q(|\mathcal{L}|)}{n\ell}$.*

Next, let

$$\lambda = \frac{\ell}{n}, \quad \Delta = \frac{D}{\ell} \text{ and } \delta = \frac{d}{n}.$$

Thus, an asymptotic version of the latter bound reads as follows.

Corollary 4.5. *The rate of the $[n, \ell, \log_q(|\mathcal{L}|), D, d]_q$ code \mathcal{L} satisfies*

$$R \leq \left(1 - \Delta - \frac{1}{n}\right) \left(1 - \delta - \lambda + \frac{1}{n}\right) + o(1).$$

4.2 Sphere-Packing Bound

Let $W_{\mathcal{L}}$ be ambient space \mathbb{F}_q^n , and let $0 \leq \ell \leq n$. Fix two integers $T \in [0, n]$, and $t \in [0, n]$. Two vector spaces $U, V \in \mathcal{P}(W_{\mathcal{L}}, \ell)$ are called (T, t) -adjacent if there exists a set of coordinates $S = \{i_1, i_2, \dots, i_s\} \subseteq [n]$, $s \leq t$, and a vector space W_S such that

$$W_{\mathcal{L}} = W_S \bigodot \langle \mathbf{e}_{i_1}, \mathbf{e}_{i_2}, \dots, \mathbf{e}_{i_s} \rangle ,$$

and

$$D(U|_{W_S}, V|_{W_S}) \leq T .$$

Note that the adjacency relation is symmetric with respect to the order of U, V , namely U and V are (T, t) -adjacent if and only if V and U are (T, t) -adjacent.

Assume that the code \mathcal{L} is used over the network. Let $U_1 \in \mathcal{L}$ be transmitted, and let the space $V \in \mathcal{P}(W_{\mathcal{L}}, \ell)$ be received as a result of T dimension erasures or gains, and t coordinate erasures. Then, U_1 and V are (T, t) -adjacent. If there is no other codeword $U_2 \in \mathcal{L}$ such that U_2 and V are (T, t) -adjacent, then the decoder, which is able to correct t coordinate erasures and T dimension erasures/gains, can recover U_1 from V . This observation motivates the following definition.

Definition 4.3. Let $W_{\mathcal{L}}$ be a vector space \mathbb{F}_q^n , and let $V \in \mathcal{P}(W_{\mathcal{L}}, \ell)$. The sphere $\mathcal{S}(V, \ell, T, t)$ around V is defined as

$$\mathcal{S}(V, \ell, T, t) = \{U \in \mathcal{P}(W_{\mathcal{L}}, \ell) : V \text{ and } U \text{ are } (T, t)\text{-adjacent}\} .$$

Now, we recall a result from [13], which we use to provide a lower bound on the number of subspaces in the sphere $\mathcal{S}(V, \ell, T, t)$.

Theorem 4.6 (Theorem 5 in [13]). For any $V \in \mathcal{P}(W_{\mathcal{L}}, \ell)$, any $0 \leq T \leq 2\ell$,

$$|\mathcal{S}(V, \ell, T, 0)| = \sum_{i=0}^{T/2} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n - \ell \\ i \end{bmatrix} .$$

We generalize this theorem in the following way.

Theorem 4.7. Let \mathcal{L} be a $[n, \ell, \log_q |\mathcal{L}|, D, d]_q$ code. For any $V \in \mathcal{L}$, any $0 \leq T \leq 2\ell$ and any $0 \leq t < d$,

$$|\mathcal{S}(V, \ell, T, t)| \geq \sum_{s=0}^t \binom{n}{s} \cdot \sum_{i=0}^{T/2} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n - s - \ell \\ i \end{bmatrix} .$$

Proof. For a particular set S of cardinality s of punctured coordinates, let $V' = V|_{W_S}$. Since $s < d$, $\dim(V') = \ell$. We also have $\dim(W_S) = n - s$. Thus,

$$|\mathcal{S}(V', \ell, T, 0)| = \sum_{i=0}^{T/2} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n - s - \ell \\ i \end{bmatrix}.$$

There are $\binom{n}{s}$ ways to choose the punctured coordinates. For each basis vector (of the row echelon form) there are q^s possibilities to fill in these missing entries. Since there are ℓ such vectors, we obtain

$$|\mathcal{S}(V, \ell, T, t)| \geq \sum_{s=0}^t \binom{n}{s} q^{\ell s} \cdot \sum_{i=0}^{T/2} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n - s - \ell \\ i \end{bmatrix}.$$

□

From Theorem 4.7, the following sphere-packing-type bound is obtained.

Corollary 4.8. *Let $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}}, \ell)$ be a code that corrects $d-1$ symbol erasures and $D-1$ dimension losses/gains. Then*

$$|\mathcal{L}| \leq \frac{|\mathcal{P}(W_{\mathcal{L}}, \ell)|}{|\mathcal{S}(V, \ell, D-1, d-1)|} \leq \frac{\begin{bmatrix} n \\ \ell \end{bmatrix}}{\sum_{s=0}^{d-1} \binom{n}{s} q^{\ell s} \cdot \sum_{i=0}^{(D-1)/2} q^{i^2} \begin{bmatrix} \ell \\ i \end{bmatrix} \begin{bmatrix} n-s-\ell \\ i \end{bmatrix}}. \quad (6)$$

Now, we turn to an asymptotic analysis of the bound (6). From Lemma 4.4, we obtain

$$|\mathcal{L}| \leq \frac{4q^{\ell(n-\ell)}}{\sum_{s=0}^{d-1} \binom{n}{s} q^{\ell s} \cdot \sum_{i=0}^{D-1} q^{i^2+i(\ell-i)+i(n-s-\ell-i)}} = \frac{4q^{\ell(n-\ell)}}{\sum_{s=0}^{d-1} \binom{n}{s} q^{\ell s} \cdot \sum_{i=0}^{D-1} q^{i(n-s-i)}}.$$

If $D-1 < (n-s)/2$, then the dominating term in $\sum_{i=0}^{D-1} q^{i(n-s-i)}$ is obtained when $i = D-1$. Similarly, if $\ell \leq n/2$, since $D-1 \leq \ell$, then clearly the dominating term in the denominator is obtained when $s = d-1$. By putting all these together we obtain that

$$\begin{aligned} |\mathcal{L}| &\leq \frac{4q^{\ell(n-\ell)}}{\binom{n}{d-1} q^{\ell(d-1)} \cdot q^{(D-1)(n-(d-1)-(D-1))}} \\ &\doteq \frac{4q^{\ell(n-\ell)}}{q^{nh_2((d-1)/n) \log_q 2 + \ell(d-1)} \cdot q^{(D-1)(n-d-D+2)}} \\ &\doteq 4q^{\ell(n-d-\ell+1) - nh_2((d-1)/n) \log_q 2 - (D-1)(n-d-D+2)}, \end{aligned}$$

where $h_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ denotes the binary entropy function, and $f(x) \doteq g(x)$ means that two expressions $f(x)$ and $g(x)$ are asymptotically equal.

By taking base- q logarithm and dividing by ℓn , we obtain the following result.

Corollary 4.9. *Let $\mathcal{L} \subseteq \mathcal{P}(W_{\mathcal{L}}, \ell)$ be a code that corrects $d-1$ symbol erasures and $D-1$ dimension losses/gains. Then, its rate satisfies:*

$$R \leq \left(1 - \delta - \lambda + \frac{1}{n}\right) - \left(\Delta - \frac{1}{\ell}\right) \left(1 - \delta - \lambda\Delta + \frac{2}{n}\right) - \left(1 - h_2\left(\delta\lambda - \frac{1}{n}\right)\right) \frac{\log_q 2}{\ell} + o(1).$$

5 Hybrid Code

Next, we construct a hybrid code, which is capable of correcting of dimension losses/gains and symbol erasures simultaneously. We show that this code is asymptotically optimal with respect to the Singleton bound. We also provide some examples discussing hybrid codes and subspace codes.

5.1 Code Construction

Let W be a vector space $(\mathbb{F}_q)^{m+\ell}$ of dimension $m+\ell$, and let \mathbb{C} be a set of subspaces of W of dimension ℓ , such that for any $U, V \in \mathbb{C}$, $V \neq U$, $\dim(U \cap V) \leq \ell - D$. We fix a basis of W , and denote its vectors by $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{m+\ell}\}$. We denote the decoder for the subspace metric and \mathbb{C} by $\mathcal{D}_{\mathbb{C}}$.

Let \mathbf{G} be a $(\ell+m) \times n$ generator matrix of the $[n, \ell+m, d]$ Generalized Reed-Solomon (GRS) code \mathcal{C} over \mathbb{F}_q of length $n \triangleq \ell+m+d-1$, given by

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdot & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{\ell+m-1} & a_2^{\ell+m-1} & a_3^{\ell+m-1} & \cdot & a_n^{\ell+m-1} \end{pmatrix} \begin{pmatrix} \eta_1 & & & & 0 \\ & \eta_2 & & & \\ & & \ddots & & \\ 0 & & & & \eta_n \end{pmatrix}.$$

Here, $a_i \in \mathbb{F}_q$, $1 \leq i \leq n$ denote n distinct nonzero field elements, and $\eta_i \in \mathbb{F}_q$, $1 \leq i \leq n$ is an arbitrary nonzero element (see [17, Chapter 5] for more details).

We use the notation \mathbf{G}_i for the i -th row of \mathbf{G} , for $i = 1, 2, \dots, \ell+m$. The code \mathcal{C} is capable of correcting any error pattern of ρ errors and μ erasures given that $2\rho + \mu \leq d-1$. In this section, we are particularly interested in the case when $\rho = 0$.

Denote by \mathcal{D}_{RS} the decoder for the code \mathcal{C} . Consider a field \mathbb{F}_{q^n} , which can also be viewed as a vector space $(\mathbb{F}_q)^n$, denoted by $W_{\mathcal{L}}$. Let \mathbf{A} be an $(\ell+m) \times (\ell+m)$ matrix over \mathbb{F}_q such that

$$\forall i = 1, 2, \dots, \ell+m : \mathbf{e}_i = \mathbf{u}_i \mathbf{A},$$

and therefore

$$\forall i = 1, 2, \dots, \ell+m : \mathbf{G}_i = \mathbf{u}_i \mathbf{A} \mathbf{G}.$$

Clearly, such an \mathbf{A} exists since $\{\mathbf{e}_i\}$ and $\{\mathbf{u}_i\}$ are two different bases for $\mathbb{F}_q^{\ell+m}$.

We define a linear mapping $\mathcal{E}_{\mathcal{L}} : W \rightarrow W_{\mathcal{L}}$ as follows. For an arbitrary vector $\mathbf{v} \in W$,

$$\mathcal{E}_{\mathcal{L}}(\mathbf{v}) = \mathbf{v}\mathbf{A}\mathbf{G}.$$

This mapping, with a slight abuse of notation, can naturally be extended to the mapping $\mathcal{E}_{\mathcal{L}} : \mathcal{P}(W) \rightarrow \mathcal{P}(\mathcal{C})$, where $\mathcal{P}(\mathcal{C})$ stands for a set of all linear sub-codes of \mathcal{C} . For any $V \in \mathcal{P}(W)$, we have

$$\mathcal{E}_{\mathcal{L}}(V) \triangleq \{\mathbf{v}\mathbf{A}\mathbf{G} : \mathbf{v} \in V\}.$$

It is easy to see that $\mathcal{E}_{\mathcal{L}}$ is a linear mapping, and that the image of the linear space V is a linear space. Moreover, it is straightforward to show that this mapping, when applied to subspaces of W , is one-to-one. Thus, for any $V \in W$,

$$\dim(V) = \dim(\mathcal{E}_{\mathcal{L}}(V)). \quad (7)$$

One can check that for any $U, V \in W$, there holds

$$\dim(U \cap V) = \dim(\mathcal{E}_{\mathcal{L}}(U) \cap \mathcal{E}_{\mathcal{L}}(V)). \quad (8)$$

Next, we define a code $\mathcal{L} \in \mathcal{P}(W_{\mathcal{L}}, \ell)$ as

$$\mathcal{L} = \{\mathcal{E}_{\mathcal{L}}(V) : V \in \mathbb{C}\}.$$

Theorem 5.1. *The code \mathcal{L} is a hybrid code over \mathbb{F}_q , with parameters $[n, \ell, |\mathbb{C}|, \geq 2D, \geq d]$.*

Proof. It is straight-forward to verify the first two parameters of \mathcal{L} . The third parameter follows from the fact that $|\mathbb{C}|$ is the number of subspaces in \mathbb{C} , and two different subspaces are mapped onto different subspaces under $\mathcal{E}_{\mathcal{L}}$.

Next, we show that \mathcal{L} is a code capable of correcting $d - 1$ symbols erasures and $D - 1$ dimension gains/losses. It suffices to show the following two properties:

1. Let $V \in \mathcal{L}$. Let V' be the subspace obtained from V by any μ symbol erasures, such that $\mu \leq d - 1$. Then, $\dim(V') = \ell$ and the space V is the only pre-image of V' in \mathcal{L} .
2. Let $U, V \in \mathcal{L}$. Let U', V' be obtained from U and V , respectively, by μ symbol erasures, such that $\mu \leq d - 1$. Here, both U and V have erasures in the same set of coordinates. Then, $\dim(U') + \dim(V') - 2 \dim(U' \cap V') \geq 2D$.

Indeed, these two conditions can be shown as follows.

1. Let $V \in \mathcal{L}$ and V' be obtained from V by μ symbol erasures, such that $\mu \leq d - 1$. Let $\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_\ell\}$ be a basis of V , and let $\{\mathbf{v}'_1, \mathbf{v}'_2, \dots, \mathbf{v}'_\ell\}$ be a set of corresponding vectors obtained by μ symbol erasures. Then, for any $a_1, a_2, \dots, a_\ell \in \mathbb{F}_q$, not all of which are zero,

$$\mathbf{v} = \sum_{i=1}^{\ell} a_i \mathbf{v}_i \in V$$

is a vector of the Hamming weight $\geq d$. Therefore, after applying μ symbol erasures, the Hamming weight of the resulting vector

$$\mathbf{v}' = \sum_{i=1}^{\ell} a_i \mathbf{v}'_i$$

is at least $d - (d - 1) \geq 1$, for any $a_1, a_2, \dots, a_\ell \in \mathbb{F}_q$, not all a_i 's are zero. Therefore, the vectors $\{\mathbf{v}'_1, \mathbf{v}'_2, \dots, \mathbf{v}'_\ell\}$ are linearly independent, and thus $\dim(V') = \ell$.

Next, take a vector $\mathbf{v}' = \sum_{i=1}^{\ell} a_i \mathbf{v}'_i \in V'$. Since the minimum distance of a code \mathcal{C} is d , and thus the code can correct any pattern of up to $d - 1$ symbol erasures, the only possible pre-image of \mathbf{v}' under any μ symbol erasures, $\mu \leq d - 1$, is $\mathbf{v} = \sum_{i=1}^{\ell} a_i \mathbf{v}_i \in V$. Therefore, each $V' \in \mathcal{L}'$ has a unique pre-image.

2. Let $U, V \in \mathcal{L}$ and let U', V' be obtained from U and V , respectively, by μ symbol erasures, such that $\mu \leq d - 1$.

From part (1) of the proof, $\dim(U') = \dim(V') = \ell$. It is sufficient to show that $\dim(U' \cap V') \leq \dim(U \cap V)$. Assume, on the contrary, that $\dim(U' \cap V') > \dim(U \cap V)$. This means that there exists $\mathbf{u} \in U$ and $\mathbf{v} \in V$, $\mathbf{u} \neq \mathbf{v}$, such that by applying μ symbol erasures, the resulting vectors \mathbf{u}' and \mathbf{v}' obtained from \mathbf{u} and \mathbf{v} , respectively, are equal. Recall, however, that $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, and therefore $d(\mathbf{u}, \mathbf{v}) \geq d$. We hence arrive to a contradiction, and thus $\dim(U') + \dim(V') - 2\dim(U' \cap V') \geq 2D$.

□

The following generalization of property 1 above holds.

Corollary 5.2. *Let V be a subcode of \mathcal{C} (of any dimension). Let V' be obtained from V by arbitrary μ symbol erasures, such that $\mu \leq d - 1$. Then, $\dim(V') = \dim(V)$ and the space V is the only pre-image of V' in $\mathcal{P}(\mathcal{C})$.*

The proof is analogous to the proof of property 1.

5.2 Asymptotic Optimality

In Section 4 we derived some upper bounds on the size of more general codes. These bounds imply upper bounds on the size of the code \mathcal{L} . Moreover, the code \mathcal{L} is asymptotically optimal with respect to one of these bounds.

Consider the code \mathcal{L} constructed from the subspace code with parameters $[m+\ell, \ell, \log_q |\mathbb{C}|, 2D]_q$ and a classical GRS code with parameters $[n, m+\ell, d]_q$, $n = \ell + m + d - 1$, as described in the previous section. The resulting code \mathcal{L} is a $[n, m+\ell, \log_q |\mathbb{C}|, 2D, d]_q$ code. The number of codewords of the code is $|\mathbb{C}|$. If we take $|\mathbb{C}|$ as described in [13], then the q -ary logarithm of the number of the codewords is given by

$$\log_q |\mathbb{C}| = m(\ell - D + 1) .$$

Therefore, the log of the cardinality of \mathcal{L} is given by

$$\log_q |\mathcal{L}| = m(\ell - D + 1) = (n - \ell - d + 1)(\ell - D + 1) . \quad (9)$$

Hence, from Lemma 4.4,

$$\frac{1}{4} \begin{bmatrix} n - d - D + 2 \\ \ell - D + 1 \end{bmatrix}_q < |\mathcal{L}| < \begin{bmatrix} n - d - D + 2 \\ \ell - D + 1 \end{bmatrix}_q .$$

Thus, the code is asymptotically order-optimal (i.e., optimal up to a constant factor) with respect to the Singleton bound (5).

5.3 Examples: Hybrid versus Subspace Codes

Let \mathcal{K} be the code defined in (2). When the code \mathcal{K} is employed over a noncoherent network, in the worst case scenario each symbol erasure translates into the loss of one dimension, and each symbol error translates into one dimension loss and one erroneous dimension gain. This may happen when all the erasures and errors occur in linearly independent vectors. In addition, note that requiring each linearly independent vector to be able to correct up to and including $d - 1$ erasures is somewhat restrictive, since it imposes an individual, rather than joint constraint, on the total number of erasures in the transmitted subspace.

We show next the advantage of using the code \mathcal{L} in the case where all data errors in the noncoherent network take form of symbol erasures. These symbol erasures are the cause of dimension losses. In this case, the code \mathcal{L} has more codewords than \mathcal{K} while having the same overall error-correcting capability.

Example 5.1. Consider the code \mathcal{K} with parameters $[m + \ell, \ell, mk, 2(\ell - k + 1)] = [6, 3, 3, 6]_q$. This code can correct up to and including two dimension losses. If the symbol erasures happen in the linearly independent vectors, the result is a loss of two dimensions,

and the code can provably correct such two symbol erasures. (Alternatively, one symbol error results in one dimension loss and one dimension gain, which is also correctable by this code.) However, this code is not able to correct any combination of three symbol erasures that occur in different basis vectors. Note that the code contains q^3 (subspaces) codewords.

Now, let $W = (\mathbb{F}_q)^4$ and consider the set $\mathcal{P} = \mathcal{P}(W, 3)$, where $|\mathcal{P}| = \begin{bmatrix} 4 \\ 3 \end{bmatrix}_q$. Fix some basis $\{\mathbf{u}_i\}_{i=1}^4$ for \mathcal{P} . Let \mathcal{C} be $[6, 4, 3]_q$ GRS code (for $q \geq 5$). Define the mapping $\mathcal{E}_{\mathcal{C}} : W \rightarrow \mathcal{C}$ as in Section 5.1.

The resulting code \mathcal{L} has

$$\begin{bmatrix} 4 \\ 3 \end{bmatrix}_q = \frac{q^4 - 1}{q - 1}$$

codewords (subspaces), for all $q \geq 5$. It has parameters $[6, 3, \log_q \left(\frac{q^4 - 1}{q - 1} \right), \geq 2, 3]_q$. Since \mathcal{C} has a minimum distance 3, \mathcal{L} can correct any two symbol erasures. If those appear in different basis vectors, the dimension loss error correcting capability matches that of the previously described subspace code. But the number of codewords in the code is strictly larger than that in \mathcal{K} .

The increase in the number of codewords achieved through hybrid coding in the above scenario is negligible for large field orders. Furthermore, even these modest advantages are present only in cases when the symbol erasures (or errors) do not appear in bursts within a few linearly independent vectors.

However, the advantage of the new construction is significantly more pronounced when the gap between ℓ and m is large. This gap becomes of interest when the length of data transmitted in the network is much higher than the dimension of the subspaces used in coding, or in other words, when the min-cut of the network is small compared to the length of the coded vectors.

Example 5.2. Take the code \mathcal{K} with parameters $[m + \ell, \ell, mk, 2(\ell - k + 1)] = [12, 4, 16, 6]_q$. This code can correct up to and including two dimension losses and it contains q^{16} codewords.

For comparison, take $W = (\mathbb{F}_q)^{10}$ and consider the set $\mathcal{P} = \mathcal{P}(W, 4)$, where $|\mathcal{P}| = \begin{bmatrix} 10 \\ 4 \end{bmatrix}_q$. Fix some basis $\{\mathbf{u}_i\}_{i=1}^{10}$ for \mathcal{P} . Let \mathcal{C} be a $[12, 10, 3]_q$ GRS code, with $q \geq 11$. Define the mapping $\mathcal{E}_{\mathcal{C}} : W \rightarrow \mathcal{C}$ as before.

The resulting code \mathcal{L} has parameters $[12, 4, \log_q \left(\begin{bmatrix} 10 \\ 4 \end{bmatrix}_q \right), \geq 2, 3]_q$. Since \mathcal{C} has a minimum distance 3, \mathcal{L} can correct any two symbol erasures.

The number of codewords in the code equals

$$\begin{bmatrix} 10 \\ 4 \end{bmatrix}_q = \frac{(q^{10} - 1)(q^9 - 1)(q^8 - 1)(q^7 - 1)}{(q^4 - 1)(q^3 - 1)(q^2 - 1)(q - 1)} > q^{24}.$$

This number is strictly larger than $4q^{16}$ (for all $q \geq 11$), which is an upper bound on the size of any $[12, 4, 16, 6]_q$ subspace code [13].

The examples described above motivate the following question: how many symbol erasures should be counted towards one dimension loss for the case that the subspace and hybrid codes have the same number of codewords?

To arrive at the desired result, we use an upper bound on the size of $\hat{\mathcal{L}}$, which was derived in [13]. Therefore, our findings are also valid for the codes constructed in [13, 21, 4], as well as for any other possible subspace code.

Let us fix the values of the parameters n and ℓ . Once again, we recall that in the worst case, each symbol erasure can cause one dimension loss. We use the Singleton bound on the size of constant-dimension codes of minimum distance $2\tilde{D}$ [13, Theorem 9]. Any such code $\hat{\mathcal{L}}$ is capable of correcting $\tilde{D} - 1$ dimension losses, so in the worst case scenario, it can provably correct only up to $\tilde{D} - 1$ symbol erasures. From [13, Theorem 9] we have

$$|\hat{\mathcal{L}}| \leq \begin{bmatrix} n - \tilde{D} + 1 \\ \ell - \tilde{D} + 1 \end{bmatrix}_q < 4q^{(\ell - \tilde{D} + 1)(n - \ell)} .$$

In comparison, the number of codewords in the code constructed in Section 5.1 is given by

$$|\mathcal{L}| = q^{(\ell - D + 1)(n - \ell - d + 1)} .$$

In order to achieve the same erasure-correcting capability, we set $\tilde{D} - 1 = (D - 1) + (d - 1)$. The underlying assumption is that $D - 1$ symbol erasures are corrected as dimensional losses, while the remaining erasures are handled as simple erasures. We require that, for small $\epsilon > 0$,

$$(\ell - (\tilde{D} - 1))(n - \ell) + \epsilon < (\ell - (D - 1))(n - \ell - (d - 1)) .$$

This is equivalent to

$$(\ell - (D - 1) - (d - 1))(n - \ell) + \epsilon < (\ell - (D - 1))(n - \ell - (d - 1)) ,$$

or

$$-(d - 1)(n - \ell) + \epsilon < -(\ell - (D - 1))(d - 1) ,$$

which reduces to

$$(n - 2\ell + (D - 1))(d - 1) > \epsilon . \tag{10}$$

The latter inequality holds for any choice of $D \geq 2$ and $d \geq 2$, when $n \geq 2\ell + \epsilon'$, for some small $\epsilon' > 0$. When the inequality (10) is satisfied, hybrid codes correct more symbol erasures than any constant-dimension subspace code, designed to correct dimension errors only.

Next, we consider maximizing the number of codewords in \mathcal{L} under the constraints that $(D - 1) + (d - 1) = \tilde{D} - 1$, and $D \geq 1$, $d \geq 1$, where \tilde{D} is fixed and D , d are allowed to vary. Recall that

$$\log_q(|\mathcal{L}|) = (\ell - (D - 1))(n - \ell - (d - 1)) .$$

Let $x \triangleq d - 1$ so that $D - 1 = s - x$, where $s = \tilde{D} - 1$ is a constant. We aim to maximize the function

$$(\ell - s + x)(n - \ell - x) . \quad (11)$$

By taking the first derivative of the expression with respect to x and by setting it to zero, we find that $x_{max} = \frac{n+s}{2} - \ell$. Therefore, the value of d that maximizes the number of codewords equals

$$d_{opt} = \frac{n + \tilde{D} + 1}{2} - \ell.$$

If $n > 2\ell$, then under the given constraints, the optimal value of d equals $d_{opt} = \tilde{D}$.

Consider the expression for the number of codewords in (11). There are two types of subspace and symbol errors considered: dimension losses and symbol erasures. A combination of such errors is termed an error pattern.

Assume that for a specific code \mathcal{L} , correcting a dimension loss is on average equivalent to correcting c symbol erasures, for some $c > 0$.

If the error pattern consists of no dimension losses and $d - 1$ symbol erasures, then (11) becomes $\ell(n - \ell - (d - 1))$. In comparison, if the error pattern consists of $D - 1$ dimension losses and no symbol erasures, then (11) becomes $(\ell - (D - 1))(n - \ell)$. Since each dimension loss is on average equivalent to c symbol erasures, we have

$$(\ell - (d/c - 1))(n - \ell) = \ell(n - \ell - (d - 1)) .$$

After applying some simple algebra, we obtain

$$\frac{1}{c} = \frac{\ell}{n - \ell} \left(1 - \frac{1}{d} \right) + \frac{1}{d} ,$$

and thus $c \approx (n - \ell)/\ell$. Therefore, vaguely speaking, it is as hard to correct one dimension loss as to correct $(n - \ell)/\ell$ symbol erasures.

6 Decoding

We proceed to present an efficient decoding procedure which handles symbol erasures, dimension losses and dimension gains. Note that the proposed decoding method may fail in the case that symbol errors are also present. This issue is discussed in more details in the Appendix.

As before, assume that $V \in \mathcal{L}$ is transmitted over a noncoherent network. Assume also that $U \in \mathcal{P}(W_{\mathcal{L}}, \ell')$, where ℓ' is not necessarily equal to ℓ , was received.

Let U' denote the vector space U , where all erased coordinates are deleted. Similarly, let \mathcal{C}' denote the code \mathcal{C} where all coordinates erased in U are deleted. We first compute

$\tilde{U}' = \mathcal{C}' \cap U'$, the intersection of U' with the subspace spanned by the code \mathcal{C}' . Assume that $\{\gamma'_1, \gamma'_2, \dots, \gamma'_{\ell''}\}$ are basis vectors of \tilde{U}' (when all erased coordinates are deleted), and $\gamma'_i \in (\mathbb{F}_q \cup \{?\})^n$. We apply the erasure-correcting GRS decoder \mathcal{D}_{RS} of the code \mathcal{C} on each γ'_i so as to obtain γ_i . Let $\tilde{U} = \langle \gamma_1, \gamma_2, \dots, \gamma_{\ell''} \rangle$. We proceed to apply the inverse of the mapping $\mathcal{E}_{\mathcal{L}}$, denoted by $\mathcal{E}_{\mathcal{L}}^{-1}$, to \tilde{U} . The resulting subspace \tilde{V} is a subspace of W , on which we now run the decoder for the code \mathcal{C} .

The algorithm described above is summarized in Figure 1.

Input: $U \subseteq (\mathbb{F}_q \cup \{?\})^n$.

Let U' be the space U , where all erased coordinates are deleted.

Let \mathcal{C}' be the code \mathcal{C} , where all coordinates erased in U are deleted.

Let $\tilde{U}' = \mathcal{C}' \cap U'$.

Denote $\tilde{U}' = \langle \gamma'_1, \gamma'_2, \dots, \gamma'_{\ell''} \rangle$.

For $i = 1, 2, \dots, \ell''$ **let** $\gamma_i = \mathcal{D}_{RS}(\gamma'_i)$.

Let $\tilde{U} = \langle \gamma_1, \gamma_2, \dots, \gamma_{\ell''} \rangle$.

Let $\tilde{V} = \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$.

Let $V_0 = \mathcal{D}_{\mathbb{C}}(\tilde{V})$.

Output: V_0 .

Figure 1: Decoder for dimension errors.

This decoder can correct any combination of Θ dimension losses and Ω dimension gains such that $\Theta + \Omega \leq D - 1$, and at most $d - 1$ symbol erasures. This is stated in the following theorem.

Theorem 6.1. *The decoder in Figure 1 can correct any error pattern of up to $d - 1$ symbol erasures and up to $D - 1$ dimension errors in \mathcal{L} .*

Proof. Suppose that $V \in \mathcal{L}$ is transmitted through the operator channel and that $U \subseteq (\mathbb{F}_q \cup \{?\})^n$ is received, where μ symbols erasures and $\Theta + \Omega$ dimension errors have occurred, such that $\mu \leq d - 1$ and $\Theta + \Omega \leq D - 1$.

We assume that the dimension errors occurred first, followed by symbol erasures. More specifically, let $S = \{j_1, j_2, \dots, j_\mu\} \subseteq [n]$ be the set of erased coordinates in U , and let

$W_{\mathcal{L}} = W_S \odot \langle e_{j_1}, e_{j_2}, \dots, e_{j_\mu} \rangle$. Then,

$$U_1 = \mathcal{H}_k(V) \oplus E \quad \text{and} \quad U' = U_1|_{W_S},$$

where $\dim(V \cap U_1) = k$, $\dim(U_1) = \ell'$, and $(\ell - k) + (\ell' - k) = \Theta + \Omega$. Here we assume that U_1 is obtained from V by applying dimension losses/gains only. We also assume that some vectors in U contain entries marked with ‘?’, and so U' is obtained by deleting those entries from all vectors in U (or, equivalently, from vectors in U_1).

Denote $V' = V|_{W_S} \subseteq \mathcal{C}'$. Then, by Lemma 2.1,

$$D(V', U') \leq D(V, U_1) \leq D - 1.$$

We have $\dim(V) = \dim(V')$, $\dim(\tilde{U}') \leq \dim(U')$. Recall that $\tilde{U}' = \mathcal{C}' \cap U'$. Therefore, since $V' \subseteq \mathcal{C}'$, we have

$$\dim(V' \cap \tilde{U}') = \dim((U' \cap \mathcal{C}') \cap V') = \dim(U' \cap (\mathcal{C}' \cap V')) = \dim(U' \cap V').$$

We consequently obtain

$$\begin{aligned} D(V', \tilde{U}') &= \dim(V') + \dim(\tilde{U}') - 2 \dim(\tilde{U}' \cap V') \\ &\leq \dim(V') + \dim(U') - 2 \dim(U' \cap V') \\ &= D(V', U') \\ &\leq D - 1. \end{aligned}$$

Observe that by Corollary 5.2, it follows that $\dim(V) = \dim(V')$ and $\dim(\tilde{U}) = \dim(\tilde{U}')$. Moreover, $\tilde{U}' \cap V'$ can be obtained from $\tilde{U} \cap V$ by μ symbol erasures. Then, according to Corollary 5.2, $\dim(\tilde{U}' \cap V') = \dim(\tilde{U} \cap V)$. We conclude that $D(V, \tilde{U}) = D(V', \tilde{U}') \leq D - 1$.

Finally, due to (7) and (8), we have that $D(\mathcal{E}_{\mathcal{L}}^{-1}(V), \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})) \leq D - 1$. Therefore, the decoder $\mathcal{D}_{\mathbb{C}}$ for the code \mathbb{C} is able to recover $\mathcal{E}_{\mathcal{L}}^{-1}(V)$, as claimed. \square

The decoding algorithms in Figure 1 consists of the following main steps:

- **Computation of the vector space $\tilde{U}' = \mathcal{L}' \cap U'$.**

Observe that $\dim(\mathcal{L}') = m + \ell$ and $\dim(U') \leq \ell'$, where $\ell' \leq \ell + D \leq 2\ell$, since otherwise the decoder cannot correct D dimensional errors. Therefore, this computation can be done by solving a system of at most n equations over \mathbb{F}_q with $m + \ell + \ell'$ unknowns. By using Gaussian eliminations, this can be done in time $O(n^2(m + \ell + \ell')) \leq O(n^2(\ell + m))$.

- **ℓ'' applications of the decoder $\mathcal{D}_{RS}(\cdot)$.**

Note that $\ell'' \leq \ell' \leq 2\ell$. This requires $O(\ell'' n \log n) \leq O(\ell n \log n)$ operations over \mathbb{F}_q .

- **One application of the mapping $\tilde{V} = \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$.**

As before, this step is equivalent to multiplying a $\ell'' \times n$ matrix representing the basis of \tilde{U} by an $n \times (m + \ell)$ transformation matrix representing the mapping $\mathcal{E}_{\mathcal{L}}^{-1}(\cdot)$. This step requires $O(\ell''(\ell + m)n) = O(\ell(\ell + m)n)$ operations over \mathbb{F}_q .

- **One application of the decoder $\mathcal{D}_{\mathcal{C}}(\cdot)$.** This takes $O(D(m + \ell)^3)$ operations over \mathbb{F}_q (see [11, Chapter 5]).

By summing up all the quantities we arrive at an expression for the total complexity of the presented algorithm of the form

$$O(n^2(\ell + m) + \ell n \log n + \ell(\ell + m)n + D(\ell + m)^3) \leq O((\ell + m)n^2 + D(\ell + m)^3)$$

operations over \mathbb{F}_q .

We note that the most time-consuming step in the decoding process for various choices of the parameters is decoding of a constant-dimension subspace code, which requires $O(D(m + \ell)^3)$ operations over \mathbb{F}_q . However, if the error pattern in a specific network contains a large number of symbol erasures, we can design the code such that D is small (say, some small constant), thus reducing the complexity of the overall decoder.

7 Acknowledgements

This research is supported by the Air Force Research Labs. The authors wish to thank Danilo Silva for helpful comments, which substantially improved the presentation in the paper.

A Correcting Dimensions and Symbol Errors

We describe next how to use the code \mathcal{L} defined in Section 5.1 for correction of error patterns that consist of dimension losses, symbol erasures and symbol substitutions. We show that the code \mathcal{L} is capable of correcting any error pattern of up to Θ dimension losses, ρ symbol errors and μ symbol erasures, whenever $\Theta \leq D - 1$ and $2\rho + \mu \leq d - 1$. However, we note that if in addition to dimension losses one also encounters dimension gains, the decoder for the code \mathcal{L} might fail. This issue is elaborated on in the second part of the Appendix.

A.1 Decoding

Henceforth, we assume that $V \in \mathcal{L}$ is transmitted over a noncoherent network and that $U \in \mathcal{P}(W_{\mathcal{L}}, \ell')$, where ℓ' is not necessarily equal to ℓ , is received.

Suppose that $\{\gamma_1, \gamma_2, \dots, \gamma_{\ell'}\}$, $\gamma_i \in (\mathbb{F}_q \cup \{?\})^n$, are some basis vectors of U . We apply the GRS decoder \mathcal{D}_{RS} for the code \mathcal{C} on all these vectors. This decoder produces the vectors $\{\beta_1, \beta_2, \dots, \beta_{\ell'}\} \in \mathcal{C}$. We denote by \tilde{U} the span of these vectors. Then, we apply the inverse of the mapping $\mathcal{E}_{\mathcal{L}}$, denoted by $\mathcal{E}_{\mathcal{L}}^{-1}$, to \tilde{U} . The resulting subspace is a subspace of W , on which the decoder for the code \mathbb{C} is applied.

The decoding algorithm can be summarized as in Figure 2.

Input: $U = \langle \gamma_1, \gamma_2, \dots, \gamma_{\ell'} \rangle$, $\gamma_i \in (\mathbb{F}_q \cup \{?\})^n$.

For $i = 1, 2, \dots, \ell'$ **let** $\beta_i = \mathcal{D}_{RS}(\gamma_i)$.

Let $\tilde{U} = \langle \beta_1, \beta_2, \dots, \beta_{\ell'} \rangle$.

Let $\tilde{V} = \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$.

Let $V_0 = \mathcal{D}_{\mathbb{C}}(\tilde{V})$.

Output: V_0 .

Figure 2: Decoder for symbol errors.

Analysis of the Decoding Algorithm

We analyze next the algorithm in Figure 2. The main result of this section is the following theorem.

Theorem A.1. *The decoder in Figure 2 can correct any error pattern in \mathcal{L} which consists of Θ dimension losses, ρ symbol errors and μ symbol erasures, whenever $\Theta \leq D - 1$ and $2\rho + \mu \leq d - 1$.*

Proof. Suppose that $V = \langle \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_{\ell} \rangle \in \mathcal{L}$ is transmitted through an operator channel, and that $U = \langle \gamma_1, \gamma_2, \dots, \gamma_{\ell'} \rangle$, $\gamma_i \in (\mathbb{F}_q \cup \{?\})^n$ is obtained by the receiver. The assumption is that Θ dimension losses, ρ symbol errors and μ symbol erasures have occurred.

Let γ_i be an arbitrary received vector, $\gamma_i \in U$. Then, γ_i can be obtained from a unique vector $\tilde{\gamma}_i \in \mathbb{F}_q^n$ by at most ρ coordinate substitutions and at most μ coordinate erasures, where

$$\tilde{\gamma}_i = \sum_{j=1}^{\ell} a_j \mathbf{v}_j ,$$

and all $a_j \in \mathbb{F}_q$, $j = 1, 2, \dots, \ell$. Since $\tilde{\gamma}_i$ is a linear combination of vectors in V , it follows that $\tilde{\gamma}_i \in \mathcal{C}$. Therefore, the decoder \mathcal{D}_{RS} is able to recover $\tilde{\gamma}_i$ from γ_i . By using the structure of the algorithm, we conclude that $\beta_i = \tilde{\gamma}_i$, and so $\tilde{U} = \langle \beta_1, \beta_2, \dots, \beta_{\ell'} \rangle$ is a subspace of V .

Since Θ dimension losses occurred, $\Theta \leq D-1$, $\dim(V) - \dim(\tilde{U}) \leq \Theta$ and $D(V, \tilde{U}) \leq D-1$. Due to (7) and (8), we have that $D(\mathcal{E}_{\mathcal{L}}^{-1}(V), \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})) \leq D-1$. Therefore, the decoder $\mathcal{D}_{\mathcal{C}}$ is able to recover $\mathcal{E}_{\mathcal{L}}^{-1}(V)$ from $\mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$, as claimed. \square

Decoding Time Complexity

The decoding algorithm consists of the following computational steps:

- **ℓ' applications of a Reed-Solomon decoder, for codes of length $n = m + \ell + d - 1$.**
By using Berlekamp-Massey type decoders, each decoder run can be performed with $O(n \log n)$ operations over \mathbb{F}_q . For this step, we hence have a total complexity of $O(\ell' n \log n)$.
- **One application of the mapping $\tilde{V} = \mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$.**
First, we have to find a basis for \tilde{U} . Gaussian elimination requires $O(\ell'^2 n)$ operations over \mathbb{F}_q . The mapping $\mathcal{E}_{\mathcal{L}}^{-1}(\tilde{U})$ is equivalent to multiplying an $\ell' \times n$ matrix representing the basis of \tilde{U} by a $n \times (m + \ell)$ transformation matrix representing the mapping $\mathcal{E}_{\mathcal{L}}^{-1}(\cdot)$. The computation of this transformation matrix is done only once in the preprocessing step, and so we may assume that this matrix is known. We hence conclude that this step takes $O(\ell'(m + \ell)n + \ell'^2 n)$ operations over \mathbb{F}_q .
- **One application of the decoder $\mathcal{D}_{\mathcal{C}}(\cdot)$.**
This takes $O(D(m + \ell)^3)$ operations over \mathbb{F}_q (see [11, Chapter 5]).

The total complexity of the presented algorithm equals

$$O(\ell' n \log n + \ell'(\ell + m)n + \ell'^2 n + D(m + \ell)^3) \leq O(Dn^3 + \ell' n^2 + \ell'^2 n)$$

operations over \mathbb{F}_q .

The number of operations depends on the dimension of the received subspace, ℓ' . It would hence be desirable to derive an upper bound on ℓ' . However, since each linearly independent vector can carry a different pattern of symbol errors, the resulting dimension of U , ℓ' , may be rather large. However, if we assume that each link to the receiver carries only one vector, ℓ' can be bounded from above by the capacity of the cut between the in-degree of the receiver. Note that the same issue arises in the context of classical subspace coding, although it was not previously addressed in the literature.

A.2 Dimension Insertion and Decoder Failure

The following example illustrates that the decoder in Figure 2 may fail in the presence of both symbol errors and dimension gains.

Let $\{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_6\} \subseteq \mathbb{F}_q^6$, $q \geq 8$, be a standard basis of W , let $\ell = 3$, and let $\mathbb{C} \subseteq W$ be a subspace code with $2D = 6$. The code \mathbb{C} is able to correct up to and including two dimension losses and/or gains. Additionally, let $\{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_6\} \in \mathbb{F}_q^8$ be a basis of a $[8, 6, 3]_q$ GRS code \mathcal{C} . The code \mathcal{C} is able to correct one symbol error. Assume, without loss of generality, that $\mathbf{u}_5 = (x_1, x_2, x_3, 0, \dots, 0) \in \mathcal{C}$ is a codeword of a minimal weight in \mathcal{C} .

Assume that the sender wants to transmit the space $Z = \langle \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \rangle$ to the receiver. According to the algorithm, the sender encodes this space as $V = \mathcal{E}_{\mathcal{L}}(Z) = \langle \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3 \rangle$, and sends the vectors $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ through the network. Assume that the vector \mathbf{u}_3 is removed, and the erroneous vector $\mathbf{z} = \mathbf{u}_4 + (x_1, 0, \dots, 0)$ is injected instead. At this point, the corresponding vector space under transmission is $\langle \mathbf{u}_1, \mathbf{u}_2, \mathbf{z} \rangle$. Then, it is plausible that $\mathbf{u}_1, \mathbf{u}_2$ and \mathbf{z} propagate further through the network due to network coding. To this end, assume that the receiver receives the following linear combinations, $\mathbf{u}_1 + \mathbf{z}$ and $\mathbf{u}_2 + \mathbf{z}$. Assume also that during the last transmission, the vector \mathbf{z} is subject to a symbol error, resulting in $\mathbf{z}' = \mathbf{u}_4 + (x_1, x_2, 0, \dots, 0)$.

The receiver applies the decoder \mathcal{D}_{RS} on these three vectors, resulting in

$$\begin{aligned}\mathcal{D}_{RS}(\mathbf{u}_1 + \mathbf{z}) &= \mathbf{u}_1 + \mathbf{u}_4 ; \\ \mathcal{D}_{RS}(\mathbf{u}_2 + \mathbf{z}) &= \mathbf{u}_2 + \mathbf{u}_4 ; \\ \mathcal{D}_{RS}(\mathbf{z}') &= \mathbf{u}_4 + \mathbf{u}_5 .\end{aligned}$$

We have that

$$\tilde{U} = \langle \mathbf{u}_1 + \mathbf{u}_4, \mathbf{u}_2 + \mathbf{u}_4, \mathbf{u}_4 + \mathbf{u}_5 \rangle ,$$

and

$$\tilde{V} = \langle \mathbf{e}_1 + \mathbf{e}_4, \mathbf{e}_2 + \mathbf{e}_4, \mathbf{e}_4 + \mathbf{e}_5 \rangle .$$

Observe that $\dim(Z \cap \tilde{V}) = 1$ and that $\mathbf{e}_1 + \mathbf{e}_2 \in Z \cap \tilde{V}$, so that the subspace distance between V and \tilde{V} is four. Therefore, the subspace decoder $\mathcal{D}_{\mathbb{C}}$ may fail when decoding Z from \tilde{V} . This situation is illustrated in Figure 3.

A.3 Decoding Strategies for Dimension Gains and Symbol Errors

To illustrate the difficulty of performing combined symbol and dimension gain error decoding of the code \mathcal{L} , below we discuss some alternative decoding strategies. We mention why these strategies, when applied to the problem at hand, do not work.

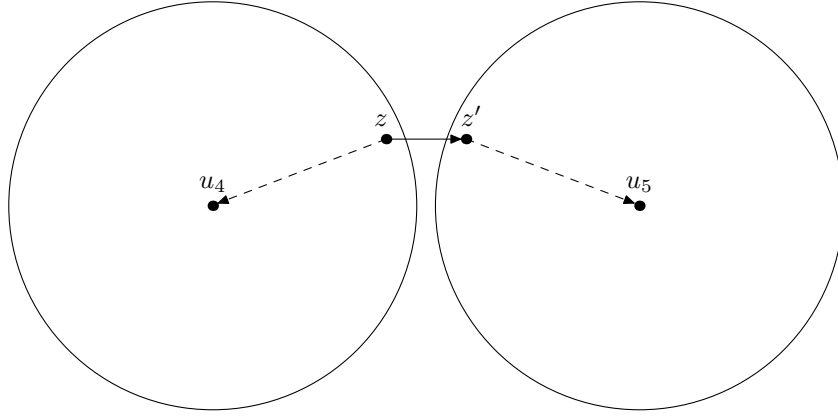


Figure 3: Situation when the decoder fails. The dimension error vector \mathbf{z} should be decoded into $\mathbf{u}_4 \in \mathcal{C}$. However, a symbol error changes \mathbf{z} into \mathbf{z}' , which is decoded into $\mathbf{u}_5 \in \mathcal{C}$. This ambiguity increases the dimension of the error space, and causes decoder failure.

Gaussian eliminations on the orthogonal space.

Assume that the vector space V is transmitted and U is obtained by a combination of symbol and dimension errors, including dimension gains. Then, U can be represented as $U = \mathcal{H}_k(V) \oplus E$, where E is some error space. If there were no symbol errors, the dimension of E would equal the number of dimension gains, which is small. However, if symbol errors are present, E takes a more involved form.

One can try to represent the space E in a particular basis, for example one in which the symbol errors have low weight. Ideally, each symbol error would correspond to a vector of weight one in that space. If one could accomplish this task, then one could find all the low weight vectors and remove them, or to puncture the corresponding coordinates. After such a procedure, one would be left with only dimension gain vectors.

A particular difficulty is that there are too many different bases for E , and it is not immediately clear which basis should be taken. And, while in the right basis the symbol error vector will have weight one, in most of the other bases this weight will be large. Moreover, the space E can be viewed as a dual code of \mathcal{L} . However, then the problem of finding low-weight vectors becomes similar to the problem of finding the smallest weight codeword in the dual code, which is known to be NP hard. Therefore, it is likely that finding the right basis in E is difficult, too.

Using list-decoding for RS codes.

One can think about using list-decoding for the code \mathcal{C} . Since the known covering radius of RS code is $d - 1$, it may happen that the dimension error will transform the codeword into a vector at distance $d - 1$ from any codeword. Then, even a single symbol error can move this codeword to a different ball of radius $d - 1$ around a codeword, similarly to the situation depicted in Figure 3. Since list-decoding can correct only less

than d errors, list-decoding cannot recover the original codeword.

The second problem associated with list decoding is as follows. Even if one could construct a polynomial-size list of all possible codewords before the dimension error took place, there would be a different list for each received vector. Since there could be as many as ℓ different lists, an exhaustive approach to picking the right codewords from all the lists would require time exponential in ℓ .

B Conclusion

We introduced a new class of subspace codes capable of correcting both dimension errors and symbol errors, termed hybrid codes. For these codes, we derived upper bounds on the size of the codes and presented an asymptotically constant-optimal concatenated code design method. We presented polynomial-time decoding algorithms which are capable of correcting the following error patterns:

- Dimension losses/gains and symbol erasures;
- Dimension losses and symbol erasures/errors.

We also discussed correction of error patterns that consist of all four types of errors: dimension losses/gains and symbol erasures/errors. As we illustrated by the example, the corresponding task is difficult, and is left as an open problem.

References

- [1] R. Ahlswede, N. Cai, S.Y.R. Li, and R.W. Yeung, “Network information flow,” *IEEE Trans. On Inform. Theory*, vol. 46, pp. 1204–1216, July 2000.
- [2] N. Cai, R. W. Yeung, “Network coding and error correction,” *Proc. IEEE Inform. Theory Workshop (ITW)*, Bangalore, India, pp. 119-122, Oct. 2002.
- [3] R. Dougherty, C. Freiling, and K. Zeger, “Insufficiency of linear coding in network information flow,” *IEEE Trans. On Inform. Theory*, vol. 51, no. 8, pp. 2745-2759, August 2005.
- [4] T. Etzion, N. Silberstein, “Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams,” *IEEE Trans. On Inform. Theory*, vol. 55, pp. 2909-2919, July 2009.
- [5] T. Etzion, A. Vardy, “Error-correcting codes in projective space,” *IEEE Trans. On Inform. Theory*, vol. 57, pp. 1165-1173, Feb. 2011.

- [6] E. M. Gabidulin, “Theory of codes with maximal rank distance,” *Problems of Information Transmission*, vol. 21, pp. 1-12, July 1985.
- [7] E.M. Gabidulin, M. Bossert, “Codes for network coding,” *Proc. IEEE Intern. Symposium on Inform. Theory (ISIT)*, Toronto, Canada, July 2008.
- [8] M. Gadouleau, Z. Yan, “Constant-rank codes and their connection to constant-dimension codes,” *IEEE Trans. On Inform. Theory*, vol. 56, no. 7, pp. 3207–3216, July 2010.
- [9] T. Ho, R. Kötter, M. Médard, D. R. Karger, and M. Effros, “The Benefits of Coding over Routing in a Randomized Setting,” *Proc. IEEE Intern. Symposium on Inform. Theory (ISIT)*, Yokohama, Japan, June-July 2003.
- [10] M. Jafari Siavoshani, S. Mohajer, C. Fragouli, and S. Diggavi, “On the capacity of non-coherent network coding,” *IEEE Trans. On Inform. Theory*, vol. 57, no. 2, pp. 1046–1066, Feb. 2011.
- [11] A. Khaleghi, D. Silva, and F. R. Kschischang, “Subspace codes,” *Lecture Notes In Computer Science*, vol. 5921, pp. 1–21, 2009.
- [12] A. Kohnert, S. Kurz, “Construction of large constant dimension codes with a prescribed minimum distance,” *Lecture Notes In Computer Science*, vol. 5393, pp. 31–42, 2008.
- [13] R. Kötter, F.R. Kschischang, “Coding for errors and erasures in random network coding,” *IEEE Trans. On Inform. Theory*, vol. 54, pp. 3579–3591, Aug. 2008.
- [14] R. Kötter, M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Transactions on Networking*, vol. 11, no. 5, pp. 782–795, October 2003.
- [15] S. Li, R. Yeung, and N. Cai, “Linear network coding,” *IEEE Trans. On Inform. Theory*, vol. 49, pp. 371–381, 2003.
- [16] F. Manganiello, E. Gorla, and J. Rosenthal, “Spread codes and spread decoding in network coding,” *Proc. IEEE Intern. Symposium on Inform. Theory (ISIT)*, Toronto, Canada, July 2008.
- [17] R. M. Roth, *Introduction to Coding Theory*, Cambridge, UK: Cambridge University Press, 2006.
- [18] R. M. Roth, “Maximum-rank array codes and their application to crisscross error correction,” *IEEE Trans. Inform. Theory*, vol. 37, pp. 328-336, March 1991.
- [19] N. Silberstein, *Coding Theory in Projective Space*, Ph.D. Research Proposal, Technion, Haifa, Israel, May 2008, available online at <http://arxiv.org/abs/0805.3528>.

- [20] D. Silva, F. R. Kschischang, and R. Kötter, “A rank-metric approach to error-control in random network coding,” *IEEE Trans. on Inform. Theory*, vol. 54, pp. 3951-3967, Sept. 2008.
- [21] V. Skachek, “Recursive code construction for random networks,” *IEEE Trans. on Inform. Theory*, vol. 56, pp. 1378-1382, March 2010.
- [22] A.-L. Trautmann, J. Rosenthal, “New improvements on the echelon-Ferrers construction,” *Proc. 19th Intern. Symposium on Math. Theory of Networks and Systems (MTNS)*, pp. 405–408, Budapest, Hungary, 2010.
- [23] S.T. Xia, F.W. Fu, “Johnson type bounds on constant dimension codes,” *Designs, Codes and Cryptography*, vol. 50, pp. 163-172, Feb. 2009.
- [24] J.H. van Lint, R.M. Wilson, *A Course in Combinatorics*, Cambridge, UK: Cambridge University Press, second ed., 2001.
- [25] H. Wang, C. Xing, and R. Safavi-Naini, “Linear authentication codes: bounds and constructions,” *IEEE Trans. On Inform. Theory*, vol. 49, pp. 866–873, Apr. 2003.